ABSTRACT OF THE DISCLOSURE

A method for power reduction and increasing computation speed for a Montgomery modulus multiplication module for performing a modulus multiplication. A coding scheme reduces the need for an adder or memory element for obtaining multiple modulus values, and the use of carry save addition with carry propagation addition increases the computational speed of the multiplication module.